In the Claims

1. – 10. (Cancel)

11. – 35. (Cancelled)

36. – 73. (Cancel)

74. (New) A method of protecting a primary memory device, comprising the steps of:

calculating a first signature of and from contents of the primary memory device comprising a verification of the contents of the primary memory device at a time the first signature is calculated;

storing the calculated signature in a secondary secure memory device separate from the primary memory device;

calculating a second signature of and from contents of the primary memory device comprising a verification of the primary memory device at a time the second signature is calculated;

comparing the first signature to the second signature; and

disconnecting the primary memory device from a control processor that operates based on instructions stored in the primary memory device if the first signature and the second signature do not match;

wherein:

the steps of calculating a first signature, storing, calculating a second signature, comparing, and disconnecting are performed by a memory protection unit that operates independently of the control processor; and

the secondary secure memory device is physically and operationally independent of the primary device.

75. (New) The method according to Claim 74, further comprising the step of maintaining stability of the control processor if the primary memory is disconnected from the control processor.

76. (New) The method according to Claim 75, wherein the step of maintaining stability of the control processor comprises placing a predetermined pattern on a data bus path to the control processor that prevents the control processor from behaving erratically.

77. (New) The method according to Claim 75, wherein the step of placing a pattern on the data bus path comprises switching the data bus path to a predetermined pattern that causes the control processor to remain in a predetermined state.

78. (New) The method according to Claim 74, wherein the memory protection unit is configured to read the contents of the primary memory device as needed for calculation of the first and second signatures but operates independently of the primary memory device; and

the secondary secure memory device operates independently of the control processor.

79. (New) The method according to Claim 74, wherein the primary memory device comprises a program memory in a consumer interactive device.

80. (New) The method according to Claim 79, wherein the consumer interactive device is a casino gaming apparatus.

81. (New) The method according to Claim 79, wherein the consumer interactive device is an ATM machine.

82. (New) The method according to Claim 79, wherein the consumer interactive device is a gaming machine and the memory protection unit is further

configured to communicate with a Remote Access Device (RAD) utilized to verify the memory contents by a floor agent according to gaming regulations.

83. (New) The method according to Claim 82, wherein the RAD includes commands usable by the floor agent to disable the gaming machine.

84. (New) The method according to Claim 83, wherein the RAD is a portable battery powered device.

85. (New) The method according to Claim 82, further comprising the step of communicating with the remote verification unit via a bluetooth communication.

86. (New) The method according to Claim 79, wherein the consumer interactive device is a casino style gaming machine and the memory protection unit further comprises a data read port coupled to the memory unit protection module and configured to communicate a verification of the memory unit to a check device external to the casino style gaming machine.

87. (New) The method according to Claim 74, wherein the secondary secure memory module is not accessible by the control processor.

88. (New) The method according to claim 74, wherein the secondary secure memory module is only accessible by the memory protection unit.

89. (New) The method according to Claim 76, wherein the predetermined pattern comprises a non-op instruction.

90. (New) The method according to Claim 74, wherein the memory protection unit is located in a memory socket in which the primary memory device is installed.

91. The method according to Claim 74, wherein the first and second signatures are calculated from the entire contents of the primary memory device.

92. (New) A method of protecting a primary memory device, comprising the steps of:

calculating a first signature of and from contents of the primary memory device comprising a verification of the contents of the primary memory device at a time the first signature is calculated;

storing the calculated signature in a secondary secure memory device separate from the primary memory device;

calculating a second signature of and from contents of the primary memory device comprising a verification of the contents of the primary memory device at a time the second signature is calculated;

comparing the first signature to the second signature;

disconnecting the primary memory device from a control processor that operates based on instructions stored in the primary memory device if the first signature and the second signature do not match;

wherein:

the steps of calculating a first signature, storing, calculating a second signature, comparing, and disconnecting are performed by a memory protection unit that operates independently of the control processor;

the secondary secure memory module is not accessible by the control processor and is physically independent of the primary memory device;

the memory protection unit is configured to read the contents of the primary memory device as needed for calculation of the first and second signatures but operates independently of the primary memory device;

the primary memory device comprises a program memory in a consumer interactive casino gaming device;

the memory protection unit is further configured to communicate with a remote verification unit utilized to verify the memory contents by a floor agent

according to gaming regulations;

the secondary secure memory module is only accessible by the memory protection unit;

the memory protection unit is located in a memory socket in which the primary memory device is installed; and

the step of disconnecting comprises physically disconnecting the primary memory device from the control processor.

93. (New) A method of protecting a program memory, comprising the steps of:

calculating a signature from contents of the program memory, the signature comprising a signature of an image of binary content of the program memory comprising a verification of the contents of the program memory; comparing the calculated signature to a previous signature of contents of the program memory from a previously known state;

preventing processor from accessing the program memory if the calculated signature does not match the previous signature;

wherein:

the steps of calculating, comparing, and preventing are performed by a memory test device;

the memory test device is operationally independent of the control device and the program memory but is capable of accessing the program memory contents;

the step of preventing comprises maintaining control device stability by placing a predetermined pattern on a control bus to the control processor to prevent erratic behavior of the control processor; and

the memory test unit comprises a unit that communicates wirelessly with a Remote Access Device (RAD) used to verify a status of the program memory.